ACTA ARITHMETICA
XLIV (1984)

An application of dihedral fields to representations of primes by binary quadratic forms

by

PIERRE KAPLAN* (Nancy), KENNETH S. WILLIAMS* (Ottawa) and YOSHIHIKO YAMAMOTO (Osaka)

1. Introduction. Let $H(m)$ denote the strict ideal class group of the quadratic field $Q(\sqrt{m})$ of discriminant m. We have

$$H(m) \simeq Z_{2^{n_1}} \times Z_{2^{n_2}} \times \ldots \times Z_{2^{n_k}} \times G, \tag{1.1}$$

where the order g of the group G is odd and Z_{2^n} denotes the cyclic group of order 2^n.

Let p be a prime number such that $\left(\frac{m}{p}\right) = 1$. Then p is represented by two inverse classes C_p, C_p^{-1} (or one ambiguous class) of binary quadratic forms of discriminant m. Gauss's theory of genera determines C_p modulo squares in the composition class group of discriminant m.

In this paper we determine the class C_p modulo fourth powers in the simplest case, namely when

$$H(m) \simeq Z_{2^n} \times G, \qquad n \geqslant 2, \tag{1.2}$$

and the class C_p is a square, that is p is a prime on which all the generic characters have the value $+1$. It is known (see for example [2]) that (1.2) occurs precisely for the following values of the discriminant m:

(I) $m = -4r$, $r\,(\text{prime}) \equiv 1 \pmod 8$;

(II) $m = -8r$, $r\,(\text{prime}) \equiv 1 \pmod 8$;

(III) $m = -8q$, $q\,(\text{prime}) \equiv 7 \pmod 8$;

(IV) $m = -qr$, $q\,(\text{prime}) \equiv 3 \pmod 4$, $r\,(\text{prime}) \equiv 1 \pmod 4$, $\left(\frac{q}{r}\right) = 1$;

(V) $m = 8r$, $r\,(\text{prime}) \equiv 1 \pmod 8$;

(VI) $m = qr$, $q\,(\text{prime}) \equiv r\,(\text{prime}) \equiv 1 \pmod 4$, $\left(\frac{q}{r}\right) = 1$.

* Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

We define
$q = 1$ in case (I),
$q = 2$ in cases (II), (V),
$r = 2$ in case (III)
and

$$k_q = \begin{cases} Q(\sqrt{-q}) & \text{in cases (I), (II), (III), (IV);} \\ Q(\sqrt{q}) & \text{in cases (V), (VI);} \end{cases}$$

$$k_r = Q(\sqrt{r}); \quad k_m = Q(\sqrt{m})$$

$$K = Q(\sqrt{r}, \sqrt{m}) = \begin{cases} Q(\sqrt{r}, \sqrt{-q}) & \text{in cases (I) to (IV),} \\ Q(\sqrt{r}, \sqrt{q}) & \text{in cases (V), (VI).} \end{cases}$$

The strict class number of the quadratic field $Q(\sqrt{d})$ will be denoted by $h(d)$.

Throughout this paper the symbol $\left(\frac{x+y\sqrt{n}}{p}\right)$, where n and x^2-ny^2 are quadratic residues of the odd prime p, will be used both as a Legendre symbol, in which case $\sqrt{n}$ is interpreted as a rational integer modulo p, as well as (equivalently) the quadratic residue symbol $\left[\frac{x+y\sqrt{n}}{P}\right]_2$ in the ring of integers of $Q(\sqrt{n})$, where P is either of the two prime ideals dividing p.
We prove:

THEOREM 1. *Let r be a prime $\equiv 1 \pmod 8$ and p a prime satisfying $\left(\frac{-1}{p}\right) = \left(\frac{p}{r}\right) = 1$, so that p is represented by the classes C_p and C_p^{-1} of discriminant $-4r$, and there exist integers a, b, e and f such that*

$$p = a^2+b^2, \tag{1.3}$$

$$p^{h(r)} = e^2-rf^2, \quad e > 0, \quad (e, f) = 1. \tag{1.4}$$

Then the class C_p is a fourth power if, and only if, for any solutions of (1.3) *and* (1.4), $\left(\frac{a+b\sqrt{-1}}{r}\right) = 1$ *or, equivalently,* $e+f \equiv 1 \pmod 4$.

THEOREM 2. *Let r be a prime $\equiv 1 \pmod 8$ and p a prime satisfying $\left(\frac{-2}{p}\right) = \left(\frac{p}{r}\right) = 1$, so that p is represented by the classes C_p and C_p^{-1} of discriminant $-8r$, and there exist integers a, b, e and f such that*

(1.5) $$p = a^2 + 2b^2,$$

(1.6) $$p^{h(r)} = e^2 - rf^2, \quad e > 0, \quad (e, f) = 1.$$

Then the class C_p *is a fourth power if, and only if, for any solutions of* (1.5) *and* (1.6), $\left(\frac{a+b\sqrt{-2}}{r}\right) = 1$ *or, equivalently,* $\left(\frac{2}{p}\right)^{(r-1)/8}\left(\frac{-2}{e+f}\right) = 1$.

THEOREM 3. *Let* $q \equiv 7 \pmod 8$ *be a prime. Let* p *be a prime satisfying* $\left(\frac{p}{q}\right) = \left(\frac{2}{p}\right) = 1$, *so that* p *is represented by the classes* C_p *and* C_p^{-1} *of discriminant* $-8q$, *and there exist integers* a, b, e *and* f *such that*

(1.7) $$p^{h(-q)} = a^2 + qb^2, \quad (a, b) = 1,\ a \text{ or } b \equiv 1 \pmod 4,$$

(1.8) $$p = e^2 - 2f^2, \quad e > 0.$$

Then the class C_p *is a fourth power if, and only if, for any solutions of* (1.7) *and* (1.8),

$$\left(\frac{-1}{p}\right)^{(q+1)/8}\left(\frac{2}{a+b}\right) = 1 \quad \text{or, equivalently,} \quad \left(\frac{e+f\sqrt{2}}{q}\right) = 1.$$

We note that Theorem 3 of [1] is part of the special case $q = 7$ of our Theorem 3.

THEOREM 4. *Let* $q \equiv 3 \pmod 4$ *and* $r \equiv 1 \pmod 4$ *be primes such that* $\left(\frac{q}{r}\right) = 1$. *Let* p *be a prime satisfying* $\left(\frac{p}{q}\right) = \left(\frac{p}{r}\right) = 1$, *so that* p *is represented by the classes* C_p *and* C_p^{-1} *of discriminant* $-qr$ *and there exist integers* a, b, e *and* f *such that*

(1.9) $$4p^{h(-q)} = a^2 + qb^2, \quad (a, b) = 1 \text{ or } 2,$$

(1.10) $$4p^{h(r)} = e^2 - rf^2, \quad (e, f) = 1 \text{ or } 2, \quad e > 0.$$

Then the class C_p *is a fourth power if, and only if, for any solutions of* (1.9) *and* (1.10),

$$\left(\frac{(a+b\sqrt{-q})/2}{r}\right) = 1 \quad \text{or, equivalently,} \quad \left(\frac{(e+f\sqrt{r})/2}{q}\right) = 1.$$

We note that Theorems 6 and 7 of [1] can be deduced as special cases of our Theorem 4 with $q = 3$, $r = 13$ and $q = 11$, $r = 5$, respectively.

THEOREM 5. *Let* r *be a prime* $\equiv 1 \pmod 8$ *and* p *be a prime satisfying* $\left(\frac{2}{p}\right)$

$=\left(\frac{p}{r}\right)=1$, *so that p is represented by the classes C_p and C_p^{-1} of discriminant $8p$, and that there exist integers a, b, e and f such that*

$$p=a^2-2b^2, \quad (a, b)=1, \quad a>0; \tag{1.11}$$

$$p^{h(r)}=e^2-rf^2, \quad (e, f)=1, \quad e+f\equiv 1 \pmod 4. \tag{1.12}$$

Then C_p is a fourth power if, and only if, for any solutions of (1.11) *and* (1.12), $\left(\frac{a+b\sqrt{2}}{r}\right)=1$ *or, equivalently,* $e+f\equiv 1 \pmod 8$.

THEOREM 6. *Let q and r be primes $\equiv 1 \pmod 4$ such that $\left(\frac{q}{r}\right)=1$. Let p be a prime satisfying $\left(\frac{p}{q}\right)=\left(\frac{p}{r}\right)=1$, so that p is represented by the classes C_p and C_p^{-1} of discriminant qr and that there exist integers a, b, e and f such that*

$$4p^{h(q)}=a^2-qb^2, \quad (a, b)=1 \text{ or } 2; \tag{1.13}$$

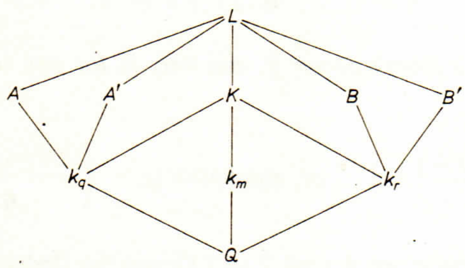
$$4p^{h(r)}=e^2-rf^2, \quad (e, f)=1 \text{ or } 2. \tag{1.14}$$

Then C_p is a fourth power if, and only if, for any solutions of (1.13) *and* (1.14),

$$\left(\frac{(a+b\sqrt{q})/2}{r}\right)=1 \quad \text{or, equivalently,} \quad \left(\frac{(e+f\sqrt{r})/2}{q}\right)=1.$$

2. Proof of the theorems. The assumption (1.2) implies that the strict class group of k_m contains exactly one subgroup of index 4. Let L be the extension of k_m corresponding to this subgroup by class field theory. Then L is the cyclic extension of degree 4 of k_m, unramified at any finite prime.

It is known ([3]) that L is a dihedral extension of Q whose quadratic subfields are k_m, k_q and k_r and whose quartic subfields are the field K, two fields A and A' containing k_q but neither k_r nor k_m, and two fields B and B' containing k_r but neither k_q nor k_m.



Let p be a prime on which all the generic characters of k_m take the value $+1$. Then p is completely decomposed in K, the genus field of k_m, and the classes C_p, C_p^{-1} are squares. The classes C_p, C_p^{-1} are fourth powers if, and only if p is completely decomposed in L, that is if p is completely decomposed in any of the four fields A, A', B or B'.

Consider for instance the extension B/k_r, of conductor f_B. There exists a character χ_B of order 2 on the group of ideals of k_r prime to f_B such that a prime ideal i of k_r is decomposed in B if, and only if, $\chi_B(i) = 1$. The value $\chi_B(i)$ is equal to $\chi_B(i^{h(r)})$, as $h(r)$ is odd, and the value of χ_B on principal ideals prime to f_B has been calculated in Propositions 2.6 to 2.11 of [4]. Applying this to either of the ideals $\bar{p}_1$, $\bar{p}_2$ such that $(p) = \bar{p}_1 \bar{p}_2$ in k_r we shall obtain the results for those theorems involving the integers e and f. The results involving the integers a and b will be obtained by considering the extension A/k_q. We give the details of the proof of Theorem 3, the other proofs are similar. In this case the decompositions of p, q and $r = 2$ in the fields k_q and k_r are the following:

$$(p) = p_1 p_2, \quad (q) = (\sqrt{-q})^2, \quad (2) = r_1 r_2 \quad \text{in } k_q, \tag{2.1}$$

$$(p) = \bar{p}_1 \bar{p}_2, \quad (q) = \bar{q}_1 \bar{q}_2, \quad 2 = (\sqrt{2})^2 \quad \text{in } k_r. \tag{2.2}$$

We first consider the extension A/k_q. By Section 2 of [4] one of r_1, r_2 is ramified in A/k_q and the other in A'/k_q; we choose the notation so that r_1 ramifies in A/k_q. By Proposition 2.9 of [4] the conductor of A/k_q is r_1^3 and the value of the character χ_A on principal ideals is given by:

$$\chi_A((\lambda)) = \left(\frac{\lambda, 2}{r_1}\right) = \begin{cases} 1, & \text{if} \quad \lambda \equiv \pm 1 \pmod{r_1^3}, \\ -1, & \text{if} \quad \lambda \equiv \pm 3 \pmod{r_1^3}. \end{cases} \tag{2.3}$$

Let (a, b) be a solution of $a^2+b^2 q = p^{h(-q)}$. As the integers $a+b\sqrt{-q}$ and $a-b\sqrt{-q}$ are coprime we may set

$$(a+b\sqrt{-q}) = p_1^{h(-q)}, \quad (a-b\sqrt{-q}) = p_2^{h(-q)}. \tag{2.4}$$

Now from (2.3) we first see, as $p \equiv \pm 1 \pmod 8$, that:

$$\chi_A(p_1)\chi_A(p_2) = \chi_A((p)) = 1, \tag{2.5}$$

so that from (2.3) and the fact that $h(-q)$ is odd:

$$\chi_A(p_1) = \chi_A(p_2) = \begin{cases} 1, & \text{if} \quad a+b\sqrt{-q} \equiv \pm 1 \pmod{r_1^3}, \\ -1, & \text{if} \quad a+b\sqrt{-q} \equiv \pm 3 \pmod{r_1^3}. \end{cases} \tag{2.6}$$

Let $\beta = 1$ or 3 be such that $q \equiv -\beta^2 \pmod{16}$. As $(\beta-\sqrt{-q})(\beta+\sqrt{-q}) \equiv 0 \pmod{r_1^4 r_2^4}$ and $(\beta-\sqrt{-q}, \beta+\sqrt{-q}) = 2$ there exists $\varepsilon = \pm 1$ such that $a+b\sqrt{-q} \equiv a+\varepsilon\beta b \pmod{r_1^3}$ and so

$$\chi_A(p_1) = \begin{cases} 1, & \text{if} \quad a+\varepsilon\beta b \equiv \pm 1 \pmod 8, \\ -1, & \text{if} \quad a+\varepsilon\beta b \equiv \pm 3 \pmod 8, \end{cases}$$

that is

$$\chi_A(p_1) = \chi_A(p_2) = \left(\frac{2}{a+\varepsilon\beta b}\right). \tag{2.7}$$

The integer a is odd or divisible by 4 according as $p \equiv 1$ or $-1 \pmod 8$ so that when $q \equiv -9 \pmod{16}$ we have

$$\left(\frac{2}{a+3b}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{a+b}\right)$$

which together with (2.7) proves

$$\chi_A(p_1) = \chi_A(p_2) = \left(\frac{-1}{p}\right)^{(q+1)/8}\left(\frac{2}{a+b}\right). \tag{2.8}$$

We next consider the extension B/k_r. By (2.1) of [4] we can suppose that q_1 ramifies in B and q_2 in B'. Then the character χ_B is given by

$$\chi_B((\lambda)) = \left[\frac{\lambda}{q_1}\right]_2 \times \operatorname{sgn} \lambda. \tag{2.9}$$

Let (e, f) be any solution of $p = e^2 - 2f^2$ where $e > 0$. Then we may set $p_1 = (e+f\sqrt{2})$, $p_2 = (e-f\sqrt{2})$, and we deduce from (2.9) that

$$\chi_B(p_1) = \chi_B(p_2) = \left[\frac{e+f\sqrt{2}}{q_1}\right]_2 = \left(\frac{e+f\sqrt{2}}{q}\right), \tag{2.10}$$

which together with (2.8) completes the proof of Theorem 3.

Remark. The class C_p of discriminant m is a fourth power or not according as $p^{h(m)/4}$ is represented by the principal class I or by the class J of order 2. Using the well-known representative of I and of J, and also the forms of discriminant $4m$ when m is odd, we obtain:

	C_p fourth power	C_p square, not fourth power
Theorem I	$p^{h(-r)/4} = X^2+rY^2$	$2p^{h(-r)/4} = X^2+rY^2$
Theorem II	$p^{h(-2r)/4} = X^2+2rY^2$	$p^{h(-2r)/4} = 2X^2+rY^2$
Theorem III	$p^{h(-2q)/4} = X^2+2qY^2$	$p^{h(-2q)/4} = 2X^2+qY^2$
Theorem IV	$\begin{cases} p^{h(-qr)/4} = X^2+XY+\frac{qr+1}{4}Y^2 \\ 4p^{h(-qr)/4} = X^2+qrY^2 \end{cases}$	$p^{h(-qr)/4} = qX^2+qXY+\frac{q+r}{4}Y^2$ $4p^{h(-qr)/4} = qX^2+rY^2$
Theorem V	$p^{h(2r)/4} = X^2-2rY^2$	$gp^{h(2r)/4} = X^2-2rY^2$
Theorem VI	$\begin{cases} p^{h(qr)/4} = X^2+XY+\frac{1-qr}{4}Y^2 \\ 4p^{h(qr)/4} = X^2-qrY^2 \end{cases}$	$gp^{h(qr)/4} = X^2+XY+\frac{1-qr}{4}Y^2$ $4gp^{h(qr)/4} = X^2-qrY^2$

In the cases (V), (VI) when $m>0$ the integer $g=-1$, q or r is such that the solvable non pellian equation is $X^2-qrY^2=g$.

Acknowledgement. We acknowledge the help of Mr. C. Frieser in calculating many numerical examples for us.

References

[1] Ezra Brown and Joseph B. Muskat, *Simultaneous representation of primes by binary quadratic forms*, Preprint.

[2] Pierre Kaplan, *Divisibilité par* 8 *du nombre des classes des corps quadratiques dont le* 2*-groupe des classes est cyclique, et réciprocité biquadratique*, J. Math. Soc. Japan 25 (1973), pp. 596–608.

[3] L. Rédei und H. Reichardt, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. 170 (1933), pp. 69–74.

[4] Yoshihiko Yamamoto, *Divisibility by* 16 *of class number of quadratic fields whose* 2*-class groups are cyclic*, Osaka Journal of Math. 21 (1984), pp. 1–22.

10, allée Jacques Offenbach
54420 Saulxures les Nancy
France

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
Ottawa, Ontario, Canada K1S 5B6

DEPARTMENT OF MATHEMATICS
OSAKA UNIVERSITY
Toyonaka, Osaka, Japan

Received on 18.10.1983 (1379)